GitHub, Inc.
Addendum: GitHub Customer Data Protection

This Data Protection Addendum ("Addendum") by and between you ("Customer", or "you") and GitHub, Inc. ("GitHub") (together, the "Parties"), is attached to and made a part of GitHub's Corporate Terms of Service Agreement effective between the Parties, including any amendments or other addenda, if applicable (together, the "Agreement"). This Addendum is made and effective as of the last date identified in the signature block (the "Addendum Effective Date"). Capitalized terms not defined in this Addendum have the meanings ascribed to them in the Agreement. In the event of a conflict or inconsistency, the terms of this Addendum will supersede those of the Agreement.

1 Definitions

1.1 The "Applicable Data Protection Laws" refer to certain laws, regulations, regulatory frameworks, or other legislations relating to the processing and use of Personal Data, as applicable to Customer's use of GitHub and the GitHub Service, including:

a. The EU General Data Protection Regulation 2016/679 ("GDPR"), along with any implementing or corresponding equivalent national laws or regulations, once in effect and applicable; and

b. The U.S. Department of Commerce and European Commission's EU–U.S. Privacy Shield Framework ("Privacy Shield"), or any succeeding legislation, available at https://www.privacyshield.gov/, or any succeeding URL, as may be amended. The "Privacy Shield Principles" refer to the principles of Notice, Choice, Accountability for Onward Transfer, Security, Data Integrity and Purpose Limitation, Access, and Recourse, Enforcement, and Liability.

1.2 "Controller," "Data Subject," "Member State," "Personal Data," "Personal Data Breach," "Processing," "Processor," and "Supervisory Authority" have the meanings given to them in the Applicable Data Protection Laws. In the event of a conflict, the meanings given in the GDPR will supersede.

1.3 "Customer Personal Data" means any Personal Data for which Customer is a Controller, whether supplied by Customer for processing by GitHub or generated by GitHub in the course of performing its obligations under the Agreement. It includes data such as billing information, IP addresses, corporate email addresses, and any other Personal Data for which Customer is a Controller.

1.4 "Customer Repository Data" means any data or information that is uploaded or created by Customer into any of its private GitHub repositories.

1.5 A "Data Breach" refers to a Personal Data Breach or any other confirmed or reasonably suspected breach of Customer's Protected Data.

1.6 "End User" means an individual Data Subject who controls a GitHub account and has agreed to the GitHub Terms of Service, and whose Personal Data is being transferred, stored, or processed by GitHub. For example, each Customer employee or contractor who has a GitHub account is also a GitHub End User.

1.7 "Permitted Purposes" for data processing are those limited and specific purposes of providing the Service as set forth in the Agreement, the GitHub Privacy Statement, and this Addendum, or the purposes for which a Data Subject has authorized the use of Customer Personal Data.

1.8 "Protected Data" includes any Customer Personal Data and any Customer Repository Data processed by GitHub on behalf of Customer under the Agreement.

1.9 “Sensitive Data” means any Personal Data revealing racial or ethnic origin; political opinions, religious or philosophical beliefs or trade union membership; processing of genetic data or biometric data for the purposes of uniquely identifying a natural person; data concerning health, a natural person’s sex life or sexual orientation; and data relating to offences, criminal convictions, or security measures.

2 Status and Compliance

2.1 Data Processing. GitHub acts as a Processor in regard to any Customer Personal Data it receives in connection with the Agreement, and GitHub will process Customer Personal Data only for Permitted Purposes in accordance with Customer’s instructions as represented by the Agreement and other written communications. In the event that GitHub is unable to comply with Customer’s instructions, such as due to conflicts with the Applicable Data Protection Laws, or where processing is required by the Applicable Data Protection Laws or other legal requirements, GitHub will notify Customer to the extent permissible. GitHub processes all Customer Personal Data in the United States or in the European Union; however, GitHub’s subprocessors may process data outside of the United States or the European Union. Additionally, GitHub acts as a Processor for any Customer Repository Data.

2.2 Data Controllers. GitHub receives Personal Data both from Customer and directly from Data Subjects who create End User accounts. Customer is a Controller only for the Customer Personal Data it transfers directly to GitHub.

2.3 GitHub Compliance. GitHub represents and warrants that it complies with Privacy Shield, which governs cross-border transfers of Personal Data. GitHub will remain certified under Privacy Shield for the duration of the Agreement, provided Privacy Shield remains a valid data transfer mechanism. In the event that GitHub is unable to remain certified, or that Privacy Shield does not remain a valid data transfer mechanism, please see Section 7. GitHub will comply with Applicable Data Protection Laws in relation to the processing of Personal Data.

3 Data Protection

3.1 Purpose Limitation. GitHub will process and communicate the Protected Data only for Permitted Purposes, unless the Parties agree in writing to an expanded purpose.

3.2 Data Quality and Proportionality. GitHub will keep the Customer Personal Data accurate and up to date, or enable Customer to do so. GitHub will take commercially reasonable steps to ensure that any Protected Data it collects on Customer’s behalf is adequate, relevant, and not excessive in relation to the purposes for which it is transferred and processed. In no event will GitHub intentionally collect Sensitive Data on Customer’s behalf. Customer agrees that the GitHub Service is not intended for the storage of Sensitive Data; if Customer chooses to upload Sensitive Data to the Service, Customer must comply with Article 9 of the GDPR, or equivalent provisions in the Applicable Data Protection Laws.

3.3 Data Retention and Deletion. Upon Customer’s reasonable request, unless prohibited by law, GitHub will return, destroy, or deidentify all Customer Personal Data and related data at all locations where it is stored after it is no longer needed for the Permitted Purposes within thirty days of request. GitHub may retain Customer Personal Data and related data to the extent required by the Applicable Data Protection Laws, and only to the extent and for such period as required by the Applicable Data Protection Laws, provided that GitHub will ensure that Customer Personal Data is processed only as necessary for the purpose specified in the Applicable Data Protection Laws and no other purpose, and Customer Personal Data remains protected by the Applicable Data Protection Laws.

3.4 Data Processing. GitHub provides the following information, required by Article 28(3) of the GDPR, regarding its processing of Customer’s Protected Data:

a. The subject matter and duration of the processing of Customer Personal Data are set out in the Agreement and this Addendum.

b. The nature and purpose of the processing of Customer Personal Data is described in Section 3.1 of this Addendum.

c. The types of Customer Personal Data to be processed are described in the GitHub Privacy Statement, and include Customer Personal Data such as user names, passwords, email addresses, and IP addresses. GitHub also processes information necessary for billing Customer’s account, but does not process or store credit card information. Customer may choose to supply

GitHub with additional Customer Personal Data, such as in Customer's profile settings or by uploading Customer Personal Data to its GitHub repositories.

d. The categories of Data Subject to whom the Customer Personal Data relates are the Customer itself and its End Users.

e. The obligations and rights of Customer are set out in the Agreement and this Addendum.

4 Security and Audit Obligations

4.1 Technical and Organizational Security Measures. Taking into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, GitHub will implement appropriate technical and organizational measures to ensure a level of security appropriate to the risks, such as against accidental or unlawful destruction, or loss, alteration, unauthorized disclosure or access, presented by processing the Protected Data. GitHub will regularly monitor compliance with these measures and will continue to take appropriate safeguards throughout the duration of the Agreement.

4.2 Incident Response and Breach Notification. GitHub will comply with the Information Security obligations in the GitHub Security Exhibit and the Applicable Data Protection Laws, including Data Breach notification obligations. Please see Section 1.2 of the GitHub Security Exhibit regarding GitHub's responsibilities in relation to Data Breach response and notification.

4.3 GitHub Personnel. GitHub represents and warrants that it will take reasonable steps to ensure that all GitHub personnel processing Protected Data have agreed to keep the Protected Data confidential and have received adequate training on compliance with this Addendum and the Applicable Data Protection Laws.

4.4 Records. GitHub will maintain complete, accurate, and up to date written records of all categories of processing activities carried out on behalf of Customer containing the information required under the Applicable Data Protection Laws. To the extent that assistance does not risk the security of GitHub or the privacy rights of individual Data Subjects, GitHub will make these records available to Customer on request as reasonably required, such as to help Customer demonstrate its compliance under the Applicable Data Protection Laws. To learn more about GitHub's requirements to provide assistance in the event of a security incident, please see Section 1.2 of the GitHub Security Exhibit.

4.5 Compliance Reporting. GitHub will provide security compliance reporting in accordance with Section 2.3 of the GitHub Security Exhibit and privacy compliance reporting in accordance with Section 2.4 of the GitHub Security Exhibit. Customer agrees that any information and audit rights granted by the Applicable Data Protection Laws (including, where applicable, Article 28(3)(h) of the GDPR) will be satisfied by these compliance reports, and will only arise to the extent that GitHub's provision of a compliance report does not provide sufficient information, or to the extent that Customer must respond to a regulatory or Supervisory Authority audit. Section 3.1 of the GitHub Security Exhibit describes the parties' responsibilities in relation to a regulatory or Supervisory Authority audit.

4.6 Assistance. GitHub will provide reasonable assistance to Customer with concerns such as data privacy impact assessments, Data Subject rights requests, consultations with Supervisory Authorities, and other similar matters, in each case solely in relation to the processing of Customer's Personal Data and taking into account the nature of processing.

5 Use and Disclosure of Protected Data

5.1 No Use in Marketing. GitHub will not use the Protected Data for the purposes of advertising third party content, and will not sell the Protected Data to any third party except as part of a merger or acquisition.

5.2 GitHub Privacy Statement. The GitHub Privacy Statement, publicly available at https://help.github.com/articles/github-privacy-statement/, provides detailed notice of GitHub's privacy and data use practices, including its use of cookies, its dispute resolution process, and further details about GitHub's GDPR compliance.

6 Subprocessing and Onward Transfer

6.1 Protection of Data. GitHub is liable for onward transfers of Protected Data to its subprocessors, such as its third party payment processor. In the event that GitHub does transfer the Protected Data to a third party subprocessor, or GitHub installs, uses, or enables a third party or third party services to process the Protected Data on GitHub's behalf, GitHub will ensure that the third party subprocessor is contractually bound to comply with or provide at least the same level of confidentiality, security, and privacy protection as is required of subprocessors by the Privacy Shield Principles and the Applicable Data Protection Laws.

6.2 Acceptance of GitHub Subprocessors. Customer authorizes GitHub to appoint (and permit each subprocessor appointed in accordance with this Section 6 to appoint) subprocessors in accordance with Section 6 and any other restrictions in the Agreement. GitHub may continue to use those subprocessors currently engaged as of the Effective Date of this Addendum.

6.3 General Consent for Onward Subprocessing. Customer provides a general consent for GitHub to engage onward subprocessors, conditional on GitHub's compliance with the following requirements:

a. Any onward subprocessor must agree in writing to only process data in a country that the European Commission has declared to have an "adequate" level of protection; or to only process data on terms equivalent to the Standard Contractual Clauses, or pursuant to a Binding Corporate Rules approval granted by competent European data protection authorities, or pursuant to a compliant US-EU Privacy Shield certification; and

b. GitHub will restrict the onward subprocessor's access to Customer Personal Data only to what is strictly necessary to perform its services, and GitHub will prohibit the subprocessor from processing the Customer Personal Data for any other purpose.

6.4 Disclosure of Subprocessor Agreements. GitHub maintains a list of onward subprocessors it has engaged to process Customer Personal Data at https://help.github.com/articles/github-subprocessors-and-cookies/, including the categories of Customer Personal Data processed, a description of the type of processing the subprocessor performs, and the location of its processing. GitHub will, upon Customer's written request, provide Customer with this list of subprocessors and the terms under which they process the Customer Personal Data. Pursuant to subprocessor confidentiality restrictions, GitHub may remove any confidential or commercially sensitive information before providing the list and the terms to Customer. In the event that GitHub cannot disclose confidential or sensitive information to Customer, the Parties agree that GitHub will provide all information it reasonably can in connection with its subprocessing agreements.

6.5 Objection to Subprocessors. GitHub will provide thirty days' prior written notice of the addition or removal of any subprocessor, including the categories listed in Section 6.4, by announcing changes on its https://github.com/github/site-policy site. If Customer has a reasonable objection to GitHub's engagement of a new subprocessor, Customer must notify GitHub promptly in writing. Where possible, GitHub will use commercially reasonable efforts to provide an alternative solution to the affected Service to avoid processing of data by the objectionable subprocessor. In the event that GitHub is unable to provide an alternative solution and the Parties cannot resolve the conflict within ninety days, Customer may terminate the Agreement.

7 Termination

7.1 Suspension. In the event that GitHub is in breach of its obligations to maintain an adequate level of security or privacy protection, Customer may temporarily suspend the transfer of all Customer Personal Data or prohibit collection and processing of Customer Personal Data on Customer's behalf until the breach is repaired or the Agreement is terminated.

7.2 Termination With Cause. In addition to any termination rights Customer has under the Agreement, Customer may terminate the Agreement without prejudice to any other claims at law or in equity in the event that:

a. GitHub notifies Customer that it can no longer meet its privacy obligations;

b. the transfer, collection, or processing of all Customer Personal Data has been temporarily suspended for longer than one month pursuant to Section 7.1;

c. GitHub is in substantial or persistent breach of any warranties or representations under this Addendum;

d. GitHub is no longer carrying on business, is dissolved, enters receivership, or a winding up order is made on behalf of GitHub; or

e. Customer objects to a subprocessor pursuant to Section 6.5, and GitHub has not been able to provide an alternative solution within ninety days.

7.3 Breach. Failure to comply with the material provisions of this Addendum is considered a material breach under the Agreement.

7.4 Failure to perform. In the event that changes in law or regulation render performance of this Addendum impossible or commercially unreasonable, the Parties may renegotiate the Addendum in good faith. If renegotiation would not cure the impossibility, or if the Parties cannot reach an agreement, the Parties may terminate the Agreement after thirty days.

7.5 Notification. In the event that GitHub determines that it can no longer meet its privacy obligations under this Addendum, GitHub will notify Customer in writing immediately.

7.6 Modifications. GitHub may modify this Addendum from time to time as required by the Applicable Data Protection Laws, with thirty days' notice to Customer.

7.7 Termination Requirements. Upon Termination, GitHub must:

a. take reasonable and appropriate steps to stop processing the Customer Personal Data;

b. within ninety days of termination, delete or deidentify any Customer Personal Data GitHub stores on Customer's behalf pursuant to Section 3.3; and

c. provide Customer with reasonable assurance that GitHub has complied with its obligations in Section 7.7.

8 Liability for Data Processing

8.1 Limitations. Except as limited by the Applicable Data Protection Laws, any claims brought under this Addendum will be subject to the terms of the Agreement regarding Limitations of Liability.

Signed:

On behalf of GitHub:

DocuSigned by:
Tal Niv
438152A3307847C...
____
Tal Niv
VP, Law and Policy
88 Colin P. Kelly St.
San Francisco, CA 94107

September 21, 2018_________
Date

On behalf of Customer:

____
[Name]
[Title]

____
Effective Date

Addendum: GitHub Security Exhibit

1 Information Technology Security Program

1.1 Security Management: Scope and Contents. Throughout the duration of the Agreement, GitHub will maintain and enforce a written information security program ("Security Program") that aligns with industry recognized frameworks; includes security safeguards reasonably designed to protect the confidentiality, integrity, availability, and resilience of Customer Protected Data; is appropriate to the nature, size, and complexity of GitHub's business operations; and complies with the Applicable Data Protection Laws and other specific information security related laws and regulations that are applicable to the geographic regions in which GitHub does business.

a. Security Officer. GitHub has designated a senior employee to be responsible for overseeing and carrying out its Security Program and for governance and internal communications regarding information security matters.

b. Security Program Changes. GitHub will provide details of any material changes to its Security Program that may adversely affect the security of any Customer Protected Data where notification is required under applicable laws and regulations.

1.2 Incident and Breach Management. Throughout the duration of the Agreement, GitHub will provide an incident and breach management program as follows:

a. Security Availability and Escalation. GitHub will maintain appropriate security contact and escalation processes on a 24-hours-per-day, 7-days-per-week basis to ensure customers and employees can submit issues to the GitHub Security team.

b. Incident Response. GitHub will maintain, as part of its Security Program, an incident response function capable of identifying, mitigating the effects of, and preventing the recurrence of Data Breaches. Upon discovering or otherwise becoming aware of a Data Breach that may put Customer Protected Data at risk, GitHub will take all reasonable measures to mitigate the harmful effects of the breach.

c. Breach Notification. GitHub will inform Customer without undue delay upon GitHub becoming aware of a Data Breach affecting Customer's Protected Data, providing Customer with sufficient information to allow it to meet any obligations under the Applicable Data Protection Laws. This notification will include a description of the Data Breach; a description of the data involved in the Data Breach; a description of GitHub's remediation steps; a description of what steps, if any, Customer can take to protect itself; and contact information for receiving more information from GitHub.

d. Breach Recovery Reporting. GitHub will retain all data related to known and reported Data Breach investigations until GitHub reasonably determines that the information is no longer needed. Upon Customer's written request and upon conclusion of the investigation, GitHub will prepare and deliver to Customer a final report that describes the effect of the Data Breach on Customer, including: (i) the extent of the Data Breach; (ii) Customer Protected Data compromised, if any; (iii) all relevant corrective actions completed; and (iv) all efforts taken to mitigate the risks of further incidents.

1.3 Due Diligence over Subcontractors and Vendors. GitHub will maintain appropriate due diligence when utilizing subcontractors and vendors. GitHub will maintain vendor audit reports and any assessment work for a minimum of three years.

1.4 Data Center Physical Safeguards. To the extent GitHub utilizes third party vendors to host production environments, GitHub will select vendors that comply with physical security controls outlined in industry standards and that issue an annual external audit report such as SOC 2 or ISO 27001 certification. All access to areas, cabinets, or racks that house telecommunications, networking devices, and other "data transmission lines" or equipment will be controlled as follows:

a. access will be controlled by badge reader at one or more entrance points;

b. doors used only as exit points will have only "one way" doorknobs or crash bar exit devices installed;

c. all doors will be equipped with door alarm contacts;

d. all exit doors will have video surveillance capability; and

e. all card access and video systems will be tied in to generator or UPS backup systems.

2 Requests for Information and Compliance Reporting

2.1 Requests for Information. Upon Customer's written request and no more than once annually, GitHub will respond to one vendor request for information to assess security and compliance risk-related information. The response will be provided in writing within thirty days of receipt of the request, pending needed clarifications of any request.

2.2 Response Contents. GitHub will include in its annual response relevant audit reports for production datacenter, IaaS, PaaS or private hosting providers, as deemed relevant by GitHub, in its sole discretion and based on data and services rendered.

2.3 GitHub Security Audit Report. GitHub commits to executing, on the earliest commercially reasonable timeline, a SOC 2, type 1 audit report, to be followed by a SOC 2, type 2 audit report, and to apply due diligence to closing audit work in a timely fashion.

2.4 GitHub Privacy Compliance Report. Upon Customer's written request and no more than once annually, GitHub will provide a privacy compliance report regarding its data privacy safeguards, without cost to Customer.

3 Cooperation with Regulatory Audits

3.1 Regulatory Audits. Should Customer realize a regulatory audit or an audit in response to a Supervisory Authority that requires participation from GitHub, GitHub will fully cooperate with related requests by providing access to relevant knowledgeable personnel, documentation, and application software. Customer has the following responsibilities regarding any such regulatory or Supervisory Authority audits:

a. Customer must ensure use of an independent third party (such as the regulator or regulator's delegate), and that findings and data not relevant to Customer are restricted.

b. Notification of such audit must be written and provided to GitHub in a timely fashion, pending regulator notification, and in a manner that allows for appropriate personnel to be made available to assist. Where regulators provide no advance notice to Customer of audit or investigation, GitHub will respond in as timely a fashion as required by regulators.

c. Any third party auditor must disclose to GitHub any findings and recommended actions where allowed by regulator.

d. In the event of a regulatory audit, access will be permitted only during regular business hours, Pacific time.

e. To the extent permitted by law, Customer must keep confidential any information gathered through any such audit of GitHub that, by its nature, should be confidential.